

State of Vermont

Backup Policy



Date: 11-02-10

Approved by: Tom Pelham

Policy Number:

Contents

1.0 Introduction	3
1.1 Authority	3
1.2 Purpose	3
1.3 Scope	4
2.0 Policy	4
2.1 Information Technology Responsibilities:	4
3.0 Policy Notification.	5

1.0 Introduction

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.”

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

Backup is a copy of a program or file that is stored separately from the original. These duplicated copies of data on different storage media or additional hardware resources are used to restore the original after a data loss event. Backups are used primarily for two purposes. The most common is to restore small numbers of files after they have been accidentally deleted or corrupted. The second is to restore a state following a disaster. Backups are not archives and are not a substitute for record retention plans, nor are they, by themselves, business continuity plans.

This policy defines the backup for computer systems that store State data.. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include file server, mail server, web server. application server and database server.

This policy is also designed to prevent the loss of State of Vermont data in the event of an equipment failure or destruction.

1.3 Scope

This policy applies to all servers and mainframes maintained by the State of Vermont. This policy does not apply to PC workstations, laptops and applicable peripherals that do not store original, or source, documents and data for the State.

For the purpose of this policy, department refers to any State entity including agencies, departments, boards and councils or other entities in the executive branch of government.

2.0 Policy

All information stored electronically in computerized form must be backed up on a routine basis to ensure its safety in the event of a severe hardware interruption, software interruption, virus attack, or other disaster. Exceptions would be servers with areas designed not to be backed up, such as those holding temporary work. Likewise, all operating software and application software necessary to access, recreate, or generate the information should also be backed up. The frequency of backup will depend on the significance of the information and its frequency of change. The most current copy of backup media should be stored off-site at an authorized location. Procedures for recovery and restoration of the information should be documented.

2.1 Information Technology Responsibilities:

Below are guidelines of procedures and responsibilities for defined information technology (IT) employees (i.e., IT managers, system administrators, network administrators). These guidelines will include a backup strategy that applies to the following:

- Identify computerized systems that store source or original State information.
- Implement standard frequency and type of backup for each type of computer system or platform in use based on the significance of the information and its frequency of change.
 - Backups should occur on a daily basis or be based on the significance of the information and its frequency of change. A preferred method of backup is disk-to-disk backup. If this method is not applicable for the system, then tape backup is required.
 - Back up all necessary data files and programs to recreate the operating environment.

- Implement procedures for transferring a recent copy of backup media to a physically and environmentally secure off-site storage location. An inventory and tracking system must be maintained. Ensure that the following are stored at the off-site storage location:
 - ✓ Source and object code for production programs
 - ✓ Master files and transaction files necessary to recreate the current master files
 - ✓ System and program documentation
 - ✓ Operating systems, utilities, and other environmental software
 - ✓ Other vital records
- Ensure that documented procedures exist for the recovery and restoration of information from backup media.
- Identify I.T. staff responsible for ensuring successful back-ups.
- Routinely copy operating software, application software, and production information to backup media based on frequencies set by management. This applies to major systems (e.g., local area network (LAN) or wide area network (WAN) servers, client/server database servers, special-purpose computers) in use by State of Vermont agencies and departments.
- Maintain at least three generations of backup media, i.e. “grandfather, father, son” arrangement for operating and application software.
- Define data model to be used for each type of data; i.e. full + incremental, full + differential, (for file servers) or database exports or extracts (for applications)
- Back up of the printed documentation and preprinted forms necessary for recovery. Convert printed documentation and preprinted forms into electronic format and move them into the DR site.
- Test the backup to determine if data files and programs can be recovered

3.0 Policy Notification.

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.